der Bundeswehr
Universität München

# Secret Sharing

Seminararbeit von
Henning Hontheim
Matrikelnummer: 1174049

| | |
|---|---|
| Bei: | Prof. Dr. Cornelius Greither<br>Dr. Alessandro Cobbe |
| Seminar: | Zahlentheorie und Kryprographie |
| Präsentation: | 10. März 2020 |

Universität der Bundeswehr München
Fakultät für Informatik

# Inhaltsverzeichnis



Allein aus Gründen der Lesbarkeit wird auf die gleichzeitige Verwendung mehrerer geschlechtsspezifischer Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten für alle Geschlechter.

# 1 Wozu Secret Sharing?

Arbeiten Sie mit anderen an einem geheimen Projekt, so gibt es einige Herausforderungen zu meistern. Was passiert, wenn Sie Ihren Schlüssel der geheimen Daten verlieren? Haben lediglich Sie einen Zugangs-Schlüssel? Wahrscheinlich nicht. Es ist nützlich, seien es in einem Tresor verschlossene Daten, oder die privaten Schlüssel in einer PKI, wenn nicht nur Sie den einzigen Zugang besitzen.

Aber wie teilen Sie den Zugriff auf die Daten? Wenn Sie Ihren Zugangs-Schlüssel vervielfältigen würden, hätte ein Einzelner Vollzugriff. Es wäre besser, wenn es mehrere Personen benötigen würde, um Zugriff zu erhalten – idealerweise mehr als die Hälfte aller Beteiligten. Doch wie lässt es sich in der Praxis umsetzen, dass es mehrere Personen benötigt um einen privaten Schlüssel zu rekonstruieren?

Ich möchte hier eine Technik vorstellen, die es erlaubt, Geheimnisse mit anderen zu teilen: das *Secret Sharing*. Siehe [3] und [9].

## 1.1 Ein kombinatorisches Beispiel

Mehrere Wissenschaftler $N$ arbeiten zusammen an einem Geheimprojekt. Um die Dokumente geheim zu halten und um Missbrauch vorzubeugen, verschließen sie diese in einem Tresor. Nur wenn mindestens die Hälfte aller Wissenschaftler anwesend ist, soll sich der Tresor öffnen lassen. Wie viele verschiedene Schlösser $S$ muss der Tresor mindestens besitzen? Wie viele verschiedene Schlüssel $s$ muss jeder Wissenschaftler mindestens bei sich tragen? Siehe [9] nach [6], sowie [8].

**Beispiel 1.1.** Sei $N = 11$ die Anzahl aller Wissenschaftler und $n = \lceil N/2 \rceil = 6$ die Anzahl derer, die mindestens anwesend sein müssen, damit sich der Tresor öffnen lässt. Folglich muss es also für jede Teilmenge mit $k$ Wissenschaftlern, wobei $k = N - n = 5$, genau ein Schloss geben, für das keiner der $k$ Wissenschaftler einen Schlüssel besitzt. Also muss der Tresor

$$S = \binom{N}{k} = \binom{11}{5} = 462$$

verschiedene Schlösser besitzen.

Sei $W = \{w_1, w_2, \ldots w_k, w_{k+1}\}$ mit $|W| = k + 1 = 6$ die Menge von Wissenschaftlern, die mindestens benötigt wird, um den Tresor zu öffnen. Dann gibt es genau ein bestimmtes Schloss $S'$, für das keiner der Wissenschaftler aus $W \setminus w_{k+1}$ einen Schlüssel besitzt, der Wissenschaftler $w_{k+1}$ jedoch schon.

Da für jede Permutation von $k = 5$ Wissenschaftlern genau der $w_{k+1}$ existiert, der die Teilmenge $W$ „vervollständigt“, bekommt jeder Wissenschaftler

$$s = \binom{N-1}{|W|-1} = \binom{N-1}{k} = \binom{10}{5} = 252$$

Schlüssel. Das ergibt eine Gesamtanzahl an $11 \cdot 252 = 2772$ Schlüsseln. Dass dies keine praktikable Lösung des Problems ist, ist offensichtlich.

# 2 Einfaches Secret Sharing

## 2.1 Stellenweise Aufteilung des Secrets

Ein einfaches Vorgehen zur Aufteilung eines Geheimnisses wäre es, dieses nach einer gewissen Anzahl Stellen an zu trennen.

**Beispiel 2.1.** Sei $D = 14561237$ das Geheimnis, welchen unter 2 Personen aufgeteilt werden soll. Bei 8 Stellen, könnte man der ersten Person $P_1$ die ersten 4 Stellen, der zweiten Person $P_2$ die letzten 4 Stellen zuteilen.

$$D = 14561237 = \underbrace{1\,4\,5\,6}_{=:D_1}\underbrace{1\,2\,3\,7}_{=:D_2} = D_1 \cdot 10^4 + D_2$$

Der entscheidende Nachteil hierbei ist, dass die Shares[1] $D_1$ und $D_2$ Aufschluss über die Beschaffenheit von $D$ geben. Wer $D_1$ besitzt braucht nur $10^4$ Kombinationen zu testen, wohingegen ein unbeteiligter Dritter $10^8$ ausprobieren müsste.

**Forderung 2.2.** Fortan fordern wir also, dass es eine wichtige Eigenschaft der Shares sein muss, keine Informationen über das Geheimnis $D$ preiszugeben und alle Möglichkeiten von $D$ gleich wahrscheinlich sein sollen. Dies wird beschrieben durch das Prinzip der Konfusion, welches auf den Mathematiker Claude Shannon zurückzuführen ist. Siehe [10].

## 2.2 One-Time-Padding

### Vernam-Chiffre

Ein Verfahren, welches die geforderte Eigenschaft nicht verletzt, ist das sogenannte *One-Time-Padding*, kurz OTP. Dieses beruht auf der Vernam-Chiffre. Hierbei wird eine zufällige Zahl $r$ zu unserem Geheimnis $D$ addiert, wobei beide die gleiche Stellenanzahl haben müssen. [4]

[1] Shares sind die Bestandteile eines Geheimnisses, die zur Rekonstruktion dessen an die beteiligten Personen aufgeteilt werden.

**Beispiel 2.3.** Sei wieder $D = 14561237$ und ein $r_1 = 81613241$ zufällig gewählt. Nun berechnen wir $r_2 = D \oplus r_1$, wobei wir hier $\oplus$ die schriftliche Addition modulo 10 ist, die Überträge somit also vernachlässigt werden. Hier wäre beispielsweise $5 \oplus 6 = 1$.

$$\begin{array}{rll} & \texttt{14561237} & = D \\ \oplus & \texttt{81613241} & = r_1 \\ \hline & \texttt{95174478} & = r_2 \end{array}$$

Nun können wir das Geheimnis rekonstruieren, indem wir $D = r_2 \ominus r_1$ berechnen. Unsere Subtraktion $\ominus$ wird wieder modulo 10 gerechnet, ignoriert also auch hier für jede Stelle den (negativen) Übertrag. Somit wäre beispielsweise $1 \ominus 6 = +5$.

$$\begin{array}{rll} & \texttt{95174478} & = r_2 \\ \ominus & \texttt{81613241} & = r_1 \\ \hline & \texttt{14561237} & = D \end{array}$$

Wenn wir nun zwei Personen haben, die $D$ unter sich aufteilen möchten, erhält $P_1$ den Share $r_1 = 81613241$ und $P_2$ den Share $r_2 = 95174478$. Beide Shares geben keinerlei Aufschluss über die Beschaffenheit von $D$. Zusammen können $P_1$ und $P_2$ das Geheimnis jedoch rekonstruieren.

**Bemerkung 2.4.** Es soll angemerkt sein, dass die Addition modulo 10 nur eine mehrerer Möglichkeiten der Berechnung ist. Handelt es sich um binäre Zahlen liegt es nahe, die XOR[2]-Operation zu nutzen.

### Visuelle Kryptographie

Ein weiteres anschauliches Beispiel lässt sich im Bereich der Visuellen Kryptographie finden. Hier besteht das Geheimnis aus einer s/w-Grafik. Diese Grafik wird aufgeteilt und jeder Teil auf eine transparente Folie gedruckt. Wenn nun die Folien übereinandergelegt werden, erscheint die ursprüngliche Grafik. Jede einzelne Folie sieht dabei wie ein zufälliges Rauschen gleichverteilter schwarzer und weißer Pixel aus. Siehe [7] und [5].

**Beispiel 2.5.** Ein Bild (Abbildung 4) soll auf zwei Folien aufgeteilt werden. Die erste Folie wird mit einem zufälligen Muster bedruckt (Abbildung 1). Aus Gründen des Kontrasts müssen für jedes Pixel des originalen Bildes 4 Pixel (je ein $2 \times 2$-Quadrat) generiert werden. Die Folien enthalten also alle viermal so viele Pixel, wie das Original. Hierbei werden für jedes $(2 \times 2)$-Quadrat entweder die beiden Sub-Pixel oben links und unten rechts, oder die anderen beiden Sub-Pixel oben rechts und unten links schwarz eingefärbt.

[2] Exklusiv-Oder

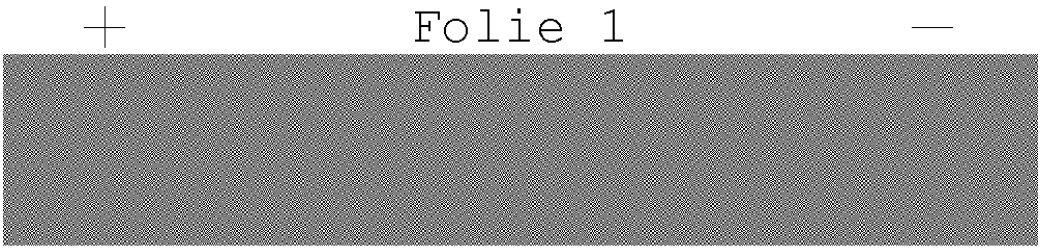



Abbildung 1: Die erste Folie mit einem zufällig generierten Muster. Von [5].

Die Pixel der zweiten Folie (Abbildung 3) werden gemäß Abbildung 2 berechnet. Wenn im Original ein schwarzes Pixel (■) vorhanden ist, muss an dieser Stelle in der zweiten Folie das Komplement der ersten Folie eingefärbt werden. Somit sind bei Überlagerung beider Folien alle 4 Sub-Pixel schwarz. Wenn das originale Pixel weiß ist (□), hat das Quadrat der zweiten Folie das gleiche Muster wie die erste Folie. Das ergibt im Schnitt ein 50%-graues Pixel (`#7F7F7F`). Weiße Pixel können über Folien nicht rekonstruiert werden, da mit den Folien keine Subtraktion möglich ist. Das ist der Grund, weshalb die Pixelanzahl vervierfacht werden muss. Siehe [5].

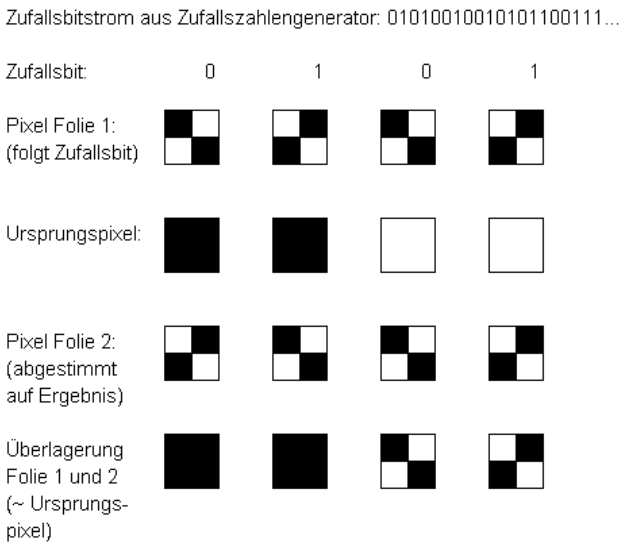



Abbildung 2: Berechnung der Pixel der zweiten Folie. Von [5].

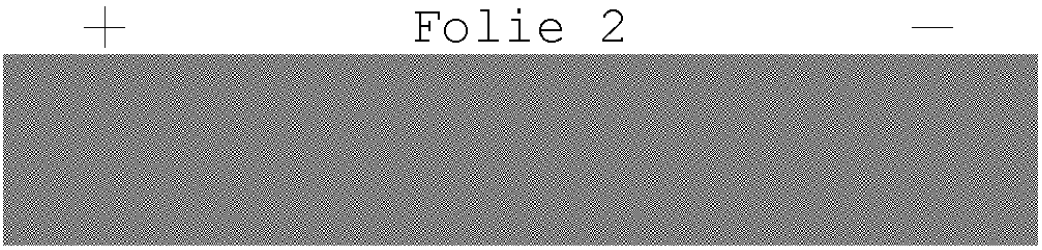



Abbildung 3: Die zweite Folie. Von [5].

Wenn nun beide Folien[3] übereinandergelegt werden, erscheint das Geheimnis:


Abbildung 4: Das mittels beider Folien rekonstruierte Geheimnis. Von [5].

#### One-Time-Padding mit mehr als 2 Personen

Wie sehen diese Verfahren aus, wenn sich mehr als zwei Personen ein Geheimnis mittels OTP teilen möchten? Auch dies ist möglich für eine beliebige Anzahl an $N$ an Personen. Doch was passiert, wenn einer der Beteiligten den eigenen Share verliert? Da alle Shares benötigt werden um das Geheimnis $D$ zu rekonstruieren, ist das unser *Single Point of Failure*. Da dies in der Praxis für große $N$ sehr schnell zu einem Problem führen kann, möchten wir dieses Verfahren hier nicht länger betrachten.

## 3 Shamir's Secret Sharing

Wir widmen uns nun einem Verfahren mit dem sich ein Geheimnis rekonstruieren lässt, ohne dass alle Shares benötigt sind. Wie im Beispiel mit den Schlössern wollen wir einen Schwellwert von Shares angeben können, die mindestens zur Rekonstruktion des Geheimnisses benötigt sein sollen. Das hier vorgestellte Secret-Sharing-Protokoll stammt von Adi Shamir. Siehe [9].

[3] Ausschnitte der Folien finden Sie in Anhang A.

Seien $n, t \in \mathbb{N}$ mit $t \leq n$. Bei diesem $(n,t)$-Secret-Sharing-Protokoll wird das Geheimnis von einem Dealer auf $n$ Personen aufgeteilt. Jeder der Geheimnisträger hat einen Teil des Geheimnisses. Wenn sich $t$ dieser Personen zusammentun, sollen sie das Geheimnis rekonstruieren können. Wenn sich aber weniger als $t$ dieser Geheimnisträger zusammentun, sollen sie keine relevante Information über das Geheimnis erhalten können. Siehe [3].

Das Verfahren beruht auf der Interpolation von Lagrange für Polynome. Haben wir $k$ verschiedene Punkte in einem zweidimensionalen Koordinatensystem $(x_1, y_1), \ldots (x_k, y_k)$ gegeben, wobei die $x_i$ paarweise verschieden sind, folgt nach dem Fundamentalsatz der Algebra, dass es genau ein Polynom $q(x)$ vom Grad $k-1$ gibt, sodass $q(x) = y_i$ für alle $i$. Siehe [9].

## 3.1 Die Vandermonde-Matrix

Bevor wir mit der Beschreibung des Protokolls beginnen können, beschäftigen wir uns mit *Vandermonde*[4]*-Matrizen.*

**Definition 3.1.** Eine Vandermonde-Matrix $V_n$ ist eine $(n \times n)$-Matrix der Form

$$V_n = \begin{pmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{pmatrix}.$$

Hierbei gilt $V_n = V(a_1, \ldots, a_n) := (v_{ij})$ mit $v_{ij} := a_i^{(j-1)}$ für $1 \leq i, j \leq n$.

**Satz 3.2.** *Die Determinante einer Vandermonde-Matrix $V_n$ ist*

$$\det V_n = \prod_{1 \leq j < i \leq n} (a_i - a_j).$$

*Beweis.* Wir beweisen dies mithilfe vollständiger Induktion gemäß [1]. Den trivialen Fall für $\det V_1 = \det\big(1\big) = 1$ vernachlässigen wir hierbei.

- **Induktionsanfang $n = 2$:**

  Der Induktionsanfang für $n = 2$ ist schnell gezeigt:

  $$\det(V_2) = \begin{vmatrix} 1 & a_1 \\ 1 & a_2 \end{vmatrix} = 1 \cdot a_2 - 1 \cdot a_1 = \prod_{j=1, i=2} (a_i - a_j) = \prod_{1 \leq j < i \leq 2} (a_i - a_j).$$

[4] nach Alexandre-Théophile Vandermonde

- **Induktionsschritt $n-1 \to n$:**

  Wir wollen dies mithilfe der Entwicklung nach Zeilen oder Spalten zeigen. Da sich dies nur empfiehlt, wenn möglichst viele Nullen in einer Zeile oder Spalte stehen, versuchen wir dies mithilfe elementarer Umformungen zu erreichen.

  Sei

$$\det V_n = \begin{vmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{vmatrix}.$$

  Um in der ersten Zeile möglichst viele Nullen zu bekommen, subtrahieren wir zunächst das $a_1$-fache der $(n-1)$-ten Spalte von der $n$-ten Spalte, dann das $a_1$-fache der $(n-2)$-ten Spalte von der $(n-1)$-ten Spalte und so weiter bis wir das $a_1$-fache der ersten Spalte von der zweiten subtrahieren. Damit erhalten wir:

$$\ldots = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & a_2 - a_1 & a_2^2 - a_1 \cdot a_2 & \cdots & a_2^{n-1} - a_1 \cdot a_2^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n - a_1 & a_n^2 - a_1 \cdot a_n & \cdots & a_n^{n-1} - a_1 \cdot a_n^{n-2} \end{vmatrix}.$$

  Dies ist noch keine Vandermonde-Matrix. Wenn wir jedoch folgende Umformung vornehmen, kommen wir unserem Ziel näher:

$$\ldots = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & (a_2 - a_1) \cdot 1 & (a_2 - a_1) \cdot a_2 & \cdots & (a_2 - a_1) \cdot a_2^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & (a_n - a_1) \cdot 1 & (a_n - a_1) \cdot a_n & \cdots & (a_n - a_1) \cdot a_n^{n-2} \end{vmatrix}.$$

  Jetzt entwickeln wir nach der ersten Spalte und erhalten:

$$\ldots = \begin{vmatrix} (a_2 - a_1) & (a_2 - a_1) \cdot a_2 & \cdots & (a_2 - a_1) \cdot a_2^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ (a_n - a_1) & (a_n - a_1) \cdot a_n & \cdots & (a_n - a_1) \cdot a_n^{n-2} \end{vmatrix}.$$

  Nun ziehen wir die Faktoren aus der Determinante heraus und bekommen:

$$\ldots = (a_2 - a_1) \cdot \ldots \cdot (a_n - a_1) \begin{vmatrix} 1 & a_2 & \cdots & a_2^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \cdots & a_n^{n-2} \end{vmatrix}.$$

Die Matrix ist nun tatsächlich eine Vandermonde-Matrix auf die wir unsere Induktionsvoraussetzung anwenden dürfen. Achtung: Die Indizes beginnen erst bei 2! Für diese $(n-1 \times n-1)$-Matrix gilt nach der Induktionsvoraussetzung:

$$\begin{vmatrix} 1 & a_2 & \cdots & a_2^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \cdots & a_n^{n-2} \end{vmatrix} = \prod_{2 \leq j < i \leq n} (a_j - a_i).$$

Daraus folgt für die Determinante einer Vandermonde-Matrix:

$$\begin{aligned} \det(V_n) = \ldots &= (a_2 - a_1) \cdot \ldots \cdot (a_n - a_1) \prod_{2 \leq j < i \leq n} (a_i - a_j) \\ &= \prod_{j=1, 1 < i \leq n} (a_i - a_j) \prod_{2 \leq j < i \leq n} (a_i - a_j) \\ &= \prod_{1 \leq j < i \leq n} (a_i - a_j). \end{aligned}$$

Damit haben wir auch den Induktionsschritt gezeigt.

□

## 3.2 Das Shamir-Secret-Sharing-Protokoll

Jetzt können wir mit der Beschreibung des Protokolls nach [3] beginnen.

**Satz 3.3.** *Seien $l, t \in \mathbb{N}, l \leq t$. Weiter seien $x_i, y_i \in \mathbb{Z}/p\mathbb{Z}, 1 \leq i \leq l$, wobei die $x_i$ paarweise verschieden sind. Dann gibt es genau $p^{t-l}$ Polynome $b \in (\mathbb{Z}/p\mathbb{Z})[X]$ vom Grad $\leq t-1$ mit $b(x_i) = y_i, 1 \leq i \leq l$, wobei $p$ eine Primzahl ist.*[5]

*Beweis.* Das Lagrange-Interpolationsverfahren liefert das Polynom

$$b(x) = \sum_{i=1}^{l} y_i \prod_{j=1, j \neq i}^{l} \frac{x_j - X}{x_j - x_i},$$

das $b(x_i) = y_i, 1 \leq i \leq l$ erfüllt und mit dem sich $b$ wieder interpolieren lässt. Jetzt muss nur noch die Anzahl dieser Polynome bestimmt werden.

Sei $b \in (\mathbb{Z}/p\mathbb{Z})[X]$ ein solches Polynom. Dieses lässt sich wie folgt darstellen:

$$b(x) = \sum_{j=0}^{t-1} b_j X^j, b_j \in \mathbb{Z}/p\mathbb{Z}, 0 \leq j \leq t-1.$$

[5] In unserem konkreten Fall gilt $l = t$.

Aus $b(x_i) = y_i, 1 \leq i \leq l$ erhält man das lineare Gleichungssystem

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{t-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{t-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_l & x_l^2 & \cdots & x_l^{t-1} \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{t-1} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_l \end{pmatrix}. \tag{1}$$

Die Teil-Koeffizientenmatrix

$$U = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{l-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{l-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_l & x_l^2 & \cdots & x_l^{l-1} \end{pmatrix}$$

ist eine Vandermonde-Matrix. Ihre Determinante ist

$$\det U = \prod_{1 \leq j < i \leq l} (x_i - x_j).$$

Weil die $x_i$ nach Voraussetzung paarweise verschieden sind, ist die Determinante ungleich Null. Der Rang von $U$ ist also $l$. Daher hat der Kern der Koeffizientenmatrix des linearen Gleichungssystems (1) den Rang $t - l$ und die Anzahl der Lösungen ist $p^{t-l}$. □

## 3.3 Berechnung der Shares

Der Dealer wählt eine Primzahl $p, p \geq n + 1$ und paarweise von Null verschiedene Elemente $x_i \in \mathbb{Z}/p\mathbb{Z}, 1 \leq i \leq n$. Die Elemente aus $\mathbb{Z}/p\mathbb{Z}$ stellen wir hier durch ihre kleinsten nicht negativen Vertreter dar. Die $x_i$ werden veröffentlicht.

Ein Geheimnis $s \in \mathbb{Z}/p\mathbb{Z}$ will vom Dealer verteilt werden. Dabei wird wie folgt vorgegangen:

1. Der Dealer wählt geheime Elemente $a_j \in \mathbb{Z}/p\mathbb{Z}, 1 \leq j \leq t - 1$ und konstruiert daraus das Polynom $a(X)$, dessen Grad $\leq t - 1$ ist:

$$a(X) = s + \sum_{j=1}^{t-1} a_j X^j. \tag{2}$$

2. Nun werden die Shares berechnet: $y_i = a(x_i), 1 \leq i \leq n$.

3. Der $i$-te Geheimnisträger erhält den Geheimnisteil $y_i, 1 \leq i \leq n$.

Das Geheimnis $s$ ist der konstante Term $a(0)$ des Polynoms $a(X)$.

**Beispiel 3.4.** Sei $n = 5, t = 3$. Der Dealer wählt $p = 17, x_i = i, 1 \leq i \leq 5$.

Das Geheimnis sei $s = 3$. Als geheime Koeffizienten des Polynoms werden $a_i = 13 + i, 1 \leq i \leq 2$ gewählt. Wir erhalten das geheime Polynom:

$$a(x) = 15X^2 + 14X + 3.$$

Die Geheimnisteile sind also:

$$\begin{array}{rcccl} y_1 & = & a(1) & = & 15 \quad , \\ y_2 & = & a(2) & = & 6 \quad , \\ y_3 & = & a(3) & = & 10 \quad , \\ y_4 & = & a(4) & = & 10 \quad , \\ y_5 & = & a(5) & = & 6 \quad . \end{array}$$

## 3.4 Rekonstruktion des Geheimnisses

Angenommen, es arbeiten $t$ Geheimnisträger zusammen. Die Shares seien $y_i = a(x_i), 1 \leq i \leq t$. Dies kann man durch Umnummerierung der Geheimnisteile immer erreichen. Hierbei ist $a(X)$ das Polynom aus (2). Jetzt gilt

$$a(X) = \sum_{i=1}^{t} y_i \prod_{j=1, j \neq i}^{t} \frac{x_j - X}{x_j - x_i}.$$

Dieses Polynom erfüllt nämlich $a(x_i) = y_i, 1 \leq i \leq t$ und nach Satz 3.3 gibt es genau ein solches Polynom vom Grad höchstens $t - 1$. Daher ist

$$s = a(0) = \sum_{i=1}^{t} y_i \prod_{j=1, j \neq i}^{t} \frac{x_j}{x_j - x_i}. \tag{3}$$

Die Formel (3) wird von den Geheimnisträgern benutzt, um das Geheimnis zu rekonstruieren.

**Beispiel 3.5.** Wir setzen das Beispiel 3.4 fort.

Die ersten drei Geheimnisträger rekonstruieren das Geheimnis. Mithilfe der Lagrange-Interpolationsformel erhalten wir:

$$\begin{aligned}
a(0) = & \sum_{i=1}^{t} y_i \prod_{j=1, j\neq i}^{t} \frac{x_j}{x_j - x_i} \\
= & \; y_1 \left( \frac{x_2}{x_2 - x_1} \cdot \frac{x_3}{x_3 - x_1} \right) \\
& + \; y_2 \left( \frac{x_1}{x_1 - x_2} \cdot \frac{x_3}{x_3 - x_2} \right) \\
& + \; y_3 \left( \frac{x_1}{x_1 - x_3} \cdot \frac{x_2}{x_2 - x_3} \right) \\
= & \; 15 \left( \frac{2}{2-1} \cdot \frac{3}{3-1} \right) + 6 \left( \frac{1}{1-2} \cdot \frac{3}{3-2} \right) + 10 \left( \frac{1}{1-3} \cdot \frac{2}{2-3} \right) \\
= & \; 15\frac{6}{2} + 6\frac{3}{-1} + 10\frac{2}{2} = 37 \bmod 17 = 3.
\end{aligned}$$

## 3.5 Sicherheit des Verfahrens

Angenommen, weniger als $t$ Geheimnisträger versuchen gemeinsam, das Geheimnis $s$ zu ermitteln. Ihre Anzahl sei $m, m < t$. Ihre Geheimnisteile seien $y_i, 1 \leq i \leq m$. Die Geheimnisträger wissen, dass das Geheimnis der konstante Term eines Polynoms $a \in \mathbb{Z}_p[X]$ vom Grad $\leq t-1$ ist, das $a(x_i) = y_i, 1 \leq i \leq m$ erfüllt. Aus Satz 3.3 erhält man das folgende Resultat:

**Lemma 3.6.** *Für jedes $s' \in \mathbb{Z}/p\mathbb{Z}$ gibt es genau $p^{t-m-1}$ Polynome $a'(X) \in (\mathbb{Z}/p\mathbb{Z})[X]$ vom Grad $\leq t-1$ mit $a'(0) = s'$ und $a'(x_i) = y_i, 1 \leq i \leq m$.*

*Beweis.* Da die $x_i$ paarweise und von Null verschieden sind, folgt die Behauptung aus Satz 3.3 mit $l = m + 1$. □

Lemma 3.6 zeigt, dass die $m$ Geheimnisträger keine Information über das Geheimnis bekommen, weil alle mögliche konstanten Terme gleich wahrscheinlich sind.

## 3.6 Graphische Beispiele

Das Verfahren kann auch graphisch dargestellt werden. Es folgen zwei Veranschaulichungen in $\mathbb{R}^2$. Beispiel 3.7 ist die eindeutige Interpolation einer

Geraden über zwei Punkte und Beispiel 3.8 die einer Parabel mittels drei Punkten.

**Beispiel 3.7** (Graphisches $(n, 2)$-Schema)**.** Unser Geheimnis ist der Punkt $S$. Wir wollen, dass es $t = 2$ beliebigen Personen aus $n$ möglich sein soll, dieses zu rekonstruieren. Das Polynom muss also vom Grad $t - 1 = 1$ sein. Wir brauchen demzufolge nur einen zufälligen Punkt $R$. In diesem Beispiel bekommen wir damit das Polynom $y(x) = -1/2 \cdot x + 400$. Das Geheimnis ist $y(0) = 400$. Beliebige zwei der drei berechneten Shares $s_1$ bis $s_3$ reichen aus, um das Polynom eindeutig zu bestimmen.

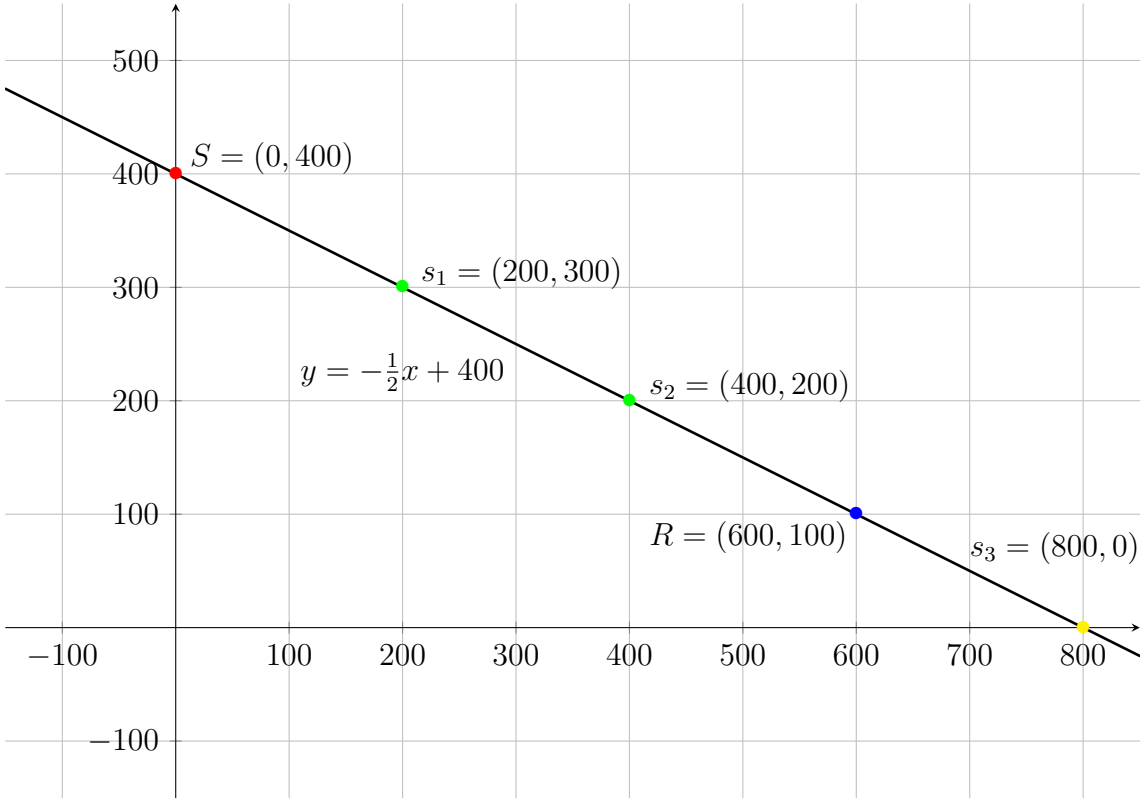



Abbildung 5: Rekonstruktion des Geheimnisses $S$ durch die Shares $s_1$ und $s_2$ mittels einer Geraden.

**Beispiel 3.8** (Graphisches $(n, 3)$-Schema)**.** Unser Geheimnis ist auch hier wieder der Punkt $S$. Nun soll es aber $t = 3$ beliebigen Personen aus $n$ möglich sein, dieses zu rekonstruieren. Das Polynom muss also vom Grad $t - 1 = 2$ sein. Wir brauchen demzufolge zwei zufällige Punkte $R_1$ und $R_2$. In diesem Beispiel bekommen wir damit das Polynom $y(x) = 1/400 \cdot x^2 - 1,75 \cdot x + 400$. Das Geheimnis ist $y(0) = 400$. Beliebige drei der vier berechneten Shares $s_1$ bis $s_4$ reichen aus, um das Polynom eindeutig zu bestimmen.

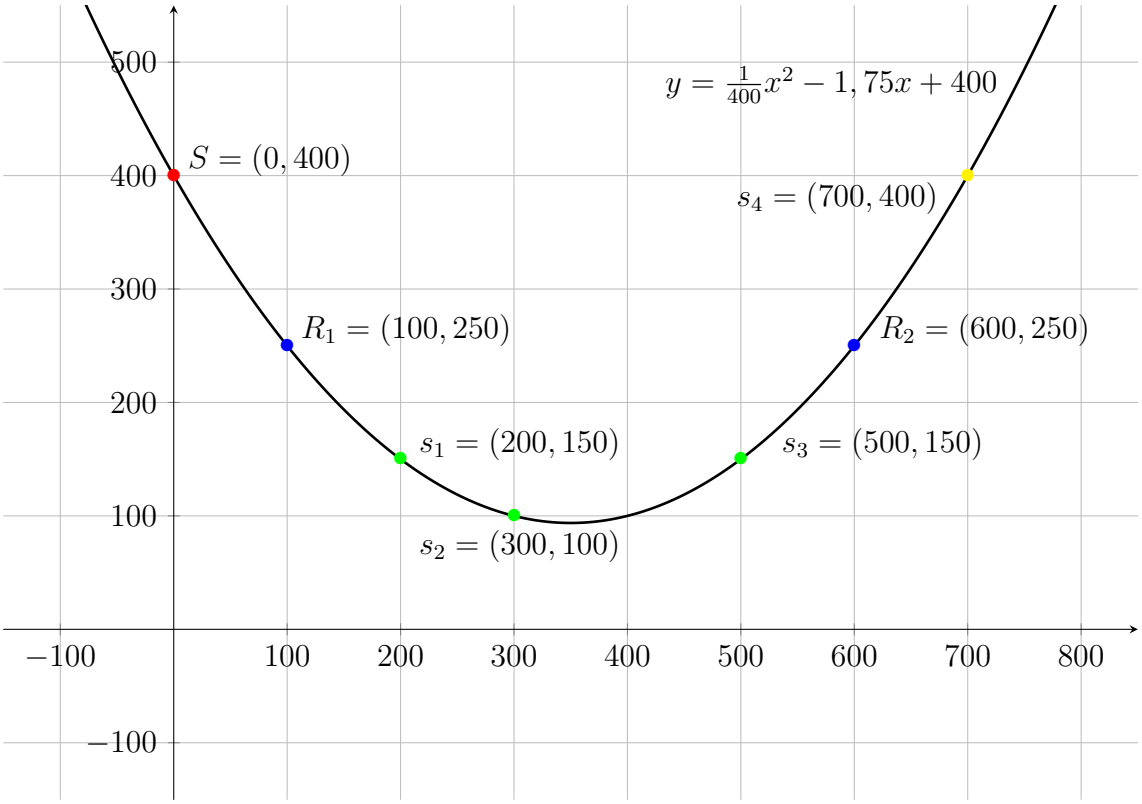



Abbildung 6: Rekonstruktion des Geheimnisses $S$ durch die Shares $s_1$ bis $s_3$ mittels einer Parabel.

## 3.7 Blakley's Secret-Sharing

George Blakley's Secret-Sharing-Protokoll hingegen basiert auf Projektiven Räumen. Der Dealer verteilt ein Geheimnis, einen Punkt, in diesem Raum mit der Dimension $k$. Jeder der $n$ Personen erhält einen Teil des Raumes der Dimension $k-1$, beispielsweise eine Hyperebene. Im Raum $\mathbb{R}^3$ schneiden sich zwei nicht parallele Geraden, die in einer gemeinsamen Ebene liegen, in genau einem Punkt. Drei nicht parallele Ebenen schneiden sich in genau einem

Punkt. Siehe Abbildung (7). Allgemein schneiden sich $n$ nicht parallele $(n-1)$-dimensionale Hyperebenen in genau einem Punkt. Wenn nun $k$ Personen Ihre Hyperebenen schneiden, erhalten sie das Geheimnis. [2][8]

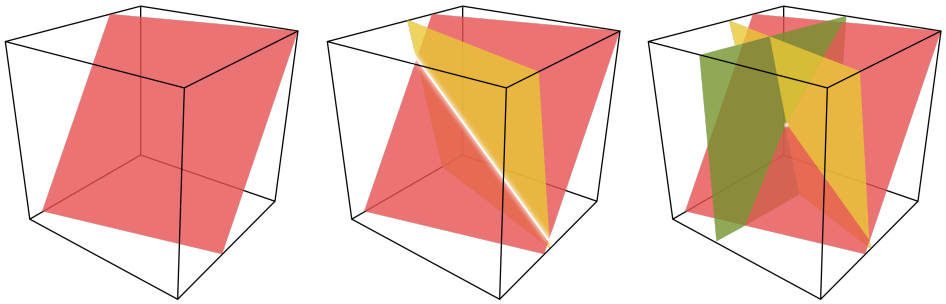


Abbildung 7: Blakley's Verfahren im $\mathbb{R}^3$: Jeder Share ist eine Ebene. Das Geheimnis ist der Punkt, in dem sich die drei Ebenen schneiden. Zwei Ebenen reichen nicht aus. Von [11].

Allerdings nehmen die Shares mehr Platz in Anspruch. Bei Shamir sind diese nicht größer, als das Geheimnis selbst. Hier sind sie $t$-mal so groß. [2]

# 4 Fazit

Shamir's Verfahren eignet sich, verglichen mit den anderen, sehr gut, um Shares zu berechnen und bringt uns gemäß [9] einige Vorteile:

1. Die Größe jedes einzelnen Shares übersteigt nicht die des Geheimnisses.

2. Wenn unser Schwellwert gleich bleibt, können wir nach Belieben Shares hinzufügen oder löschen, ohne die anderen Shares zu beeinflussen. Voraussetzung ist hier, dass es möglich sein muss, einzelne Shares vollständig zu löschen. Diese kann man beispielsweise verschlüsselt auf Chipkarten speichern.

3. Es ist sehr einfach, alle Shares auszutauschen, ohne das Geheimnis ändern zu müssen. Wir brauchen nur ein neues Polynom $a'(X)$ mit $a'(0) := a(0)$.

4. Dieses Verfahren ermöglicht es uns, eine Hierarchie unter den Geheimnisträgern zu erhalten. Geben wir beispielsweise einem Firmeninhaber drei Shares, dessen Vize-Präsidenten zwei Shares und jeder anderen Führungsperson einen Share, erlaubt es ein $(n, 3)$-Schema, die Befugnisse entsprechend der Rollen zu verteilen.

# Literaturverzeichnis


[1] Ableitinger, C., and Herrmann, A. *Lernen aus Musterlösungen zur Analysis und Linearen Algebra.* Springer Fachmedien Wiesbaden, 2013.

[2] Blakley, G. Safeguarding cryptographic keys. *Proceedings of the 1979 AFIPS National Computer Conference* (1979), 313–317.

[3] Buchmann, J. *Einführung in die Kryptographie.* Springer Berlin Heidelberg, 2016.

[4] Cobbe, A. *Zahlentheorie und Kryptographie.* Universität der Bundeswehr München, Herbsttrimester 2019.

[5] Kuhlemann, O. Visuelle Kryptografie. `http://kryptografie.de/kryptografie/chiffre/visuelle-kryptografie.htm`.

[6] Liu, C. L. *Introduction to Combinatorial Mathematics.* McGraw-Hill, New York, 1968.

[7] Naor, M., and Shamir, A. Visual cryptography. *Lecture Notes in Computer Science* (1995), 1–12.

[8] Sergienko, A. *Quantum Communications and Cryptography.* CRC Press, 01 2005.

[9] Shamir, A. How to share a secret. *Communications of the ACM 22*, 11 (Nov 1979), 612–613.

[10] Shannon, C. E. Communication Theory of Secrecy Systems. *Bell System Technical Journal 28*, 4 (1949), 656–715.

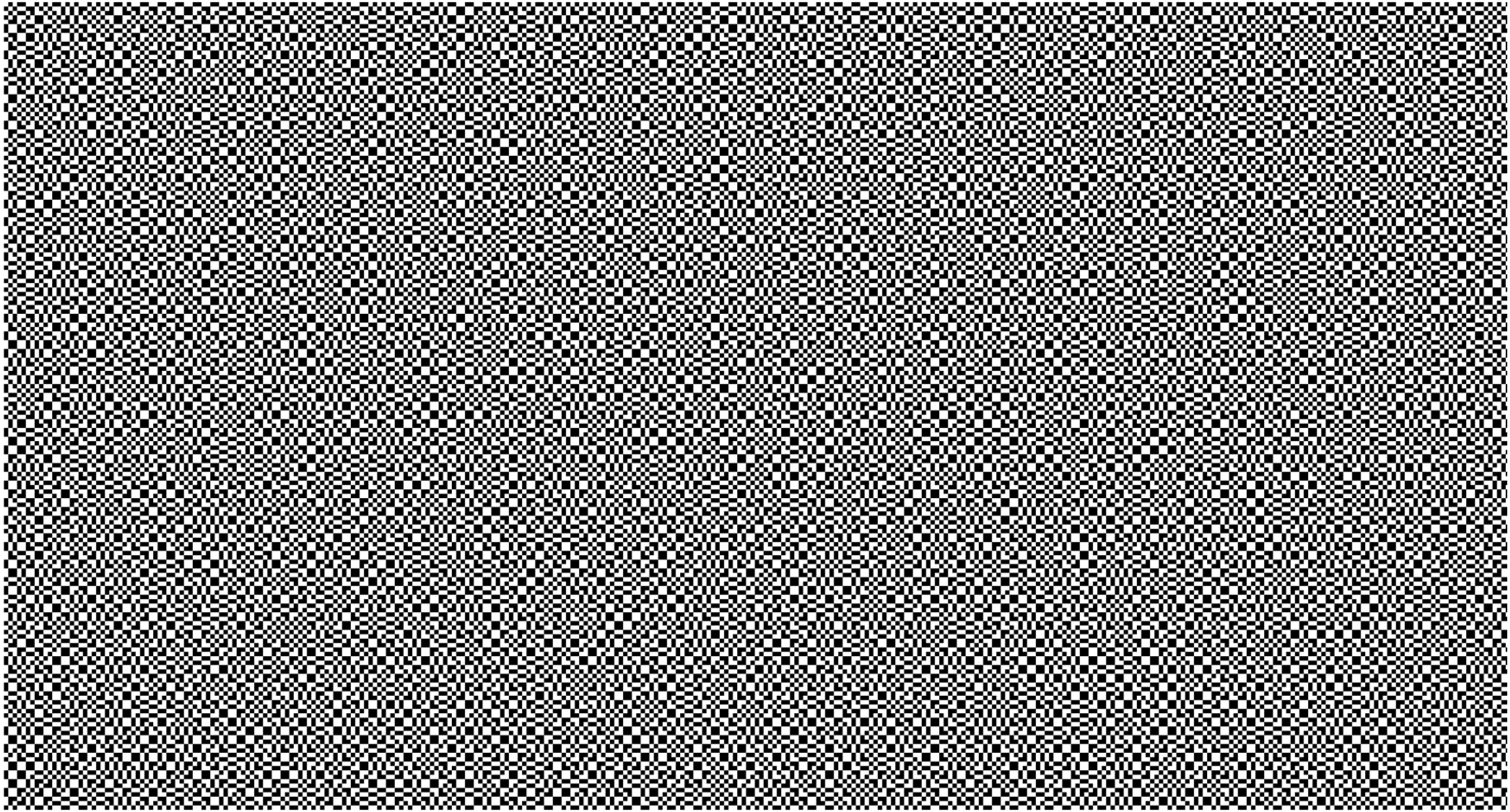
[11] the Oyster, F. Blakley's scheme. `https://en.wikipedia.org/wiki/Secret_sharing#Blakley's_scheme`.

# Anhang A

# Ausschnitte der Folien

Auf den folgenden Seiten finden Sie Ausschnitte beider in 2.5 verwendeten Folien.

Folie 1



Folie 2